PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Alfred T. TABAYOYON, JR. et al

Art Unit: 2143

Application No: 09/974,624

Examiner:
Joseph E. Avellino

Filed: October 9, 2001

For: NETWORK-BASED DOCUMENT DELIVERY SYSTEM
WITH RECEIPT AND DISPLAY VERIFICATION

BRIEF ON BEHALF OF APPELLANT

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Real Party in Interest

Swiftview, Inc.

Related Appeals and Interferences

None

Status of Claims

All claims 1-22 are rejected, no claims are withdrawn.

Status of Amendments

No amendment was filed subsequent to the last office action.

Summary of Claimed Subject Matter

Claims 1, 2, 9, 10, 13 and 14 are representative of the claimed subject matter.

Claim 1

Claim 1, best understood with reference to FIG. 1, recites a method comprises the steps of

"a. generating a document file (print file 37, FIG. 1) describing the document on [a] sender computer" (paragraph 26);

"b. sending the document file from the sender computer to [a] server computer" (paragraph 25);

"c. sending email (42, FIG. 1) to a receiver computer containing a hypertext link that the receiver activates to send a reference to the document file to the server computer" (paragraph 29);

"d. sending the document file from the server computer to the receiver computer after the server computer receives the reference to the document file from the receiver computer" (paragraph 30);

"e. processing the document file sent to the receiver computer to generate a display of an image of the document in a browser window (26, FIG. 1) on the receiver computer" (paragraph 36); and

"f. sending verification data from the receiver computer to the server computer indicating that the receiver computer has successfully displayed the image of the document in the browser window" (paragraph 34).

Claim 2

Claim 2 depends on claim 1 and recites the additional steps of

"g. storing log data on the server computer indicating when the receiver computer returned the verification data to the server computer indicating that the receiver computer has successfully displayed in the browser window the image of the document referenced by the hypertext link (paragraph 44)" ; and "h. providing the sender computer with access to the log data via the computer network (paragraph 44)."

Claim 9

Claim 9 depends on claim 1 and recites the additional step of

"g. transmitting a publish request from the sender computer to the server computer, wherein the publish request identifies the receiver computer, wherein the publish request indicates that the receiver computer is to be prevented from sending the document file to a printer (paragraph 26)."

Claim 10

Claim 10 depends on claim 9 and recites

"generating on the sender computer a print file for directing a printer to print the document, and then compressing the print file to generate the document file" (paragraph 28, lines 28-33),

"decompressing the document file to produce the print file" (paragraph 38)", and

"processing the print file to generate the display of the image of the document in the browser window on the receiver computer" (paragraph 38)".

Claim 13

Claim 3 depends on claim 1 and recites the novel additional limitation that "the receiver computer returns the verification data to the server computer as an encoded network address".

Claim 14

Referring to the drawings and specification, the invention as recited in claim 14 is a method for transmitting a document file describing a document from a sender computer to a receiver computer via a computer network linking the sender computer and the receiver computer to a server computer, wherein the sender computer is operated by a sender, wherein the receiver computer is operated by a receiver, wherein the receiver computer includes a monitor viewable by the receiver. The method comprises the steps of:

"a. transmitting the document file via the computer network from the sender computer to the server computer"; (paragraph 26)

"b. storing the document file on the server computer and assigning the document file a unique network address"; (paragraph 29)

"c. transmitting an email message via the computer network to the receiver computer, wherein the email message includes a hypertext link to the document file's assigned network address"; (paragraph 29)

"d. displaying the email message on the receiver computer monitor so that the receiver may view it and activate the hypertext link whereby the receiver computer returns the document file's network address to the server computer"; (paragraph 29)

"e. transmitting the document file from the server computer to the receiver computer via the computer network following the receiver's activation of the hypertext link"; (paragraph 30) and

"f. providing viewer software running on the receiver computer for generating a display on the receiver computer monitor of the document described by the document file when received by the receiver computer";(paragraph 36)

"wherein when the viewer software has successfully displayed the document, it automatically returns verification data in the form of an encoded network address to the server computer via the computer network verifying that the document has been successfully displayed". (paragraph 34)

Grounds For Rejection To Be Reviewed On Appeal

Grounds for rejection to be reviewed on appeal are:

1. whether claims 1-2, 4-8, 13-17 and 21 should be rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of US patent 6,789,105 (McMillan) in view of U.S. patent 6,360,254 (Linden), and U.S. patent 6,266, 703 (Clark),

2. whether claims 9, 10, and 20 should be rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of McMillan, Linden, Clark and US patent 6,209030 (Ohashi), and

3. whether claims 11, 12, 18 and 19 should be rejected under 35 U.S.C. 103(a) as being unpatentable over McMillan, Linden, Clark and U.S. patent 6,237,099 (Kurokawa).

Argument

Although the Office Action dated Feb. 24, 2006 upon which this appeal is based indicates that it is responsive to the applicant's communication filed Jan. 27, 2006, the Examiner's comments in support of rejection of the claims apparently cite language of an outdated version of the claims and do not take into account the claim amendments made in the communication dated Jan. 27, 2006. The Applicant's discussion below relative to the claim rejections is directed to the claims as amended in the response dated Jan. 27, 2006, and address the Examiner's comments to the extent they are relevant to the claims as amended.

1. **Arguments against rejection under 35 U.S.C. 103(a) as being unpatentable over the combination of McMillan, Linden, and Clark**

Claims 1, 4, 5-8, 14 - 17 and 21

McMillan (col. 3, lines 20-29) teaches that a server computer embeds code for generating a rich media display in email that a receiver computer automatically executes upon opening the email to produce the rich media display on the receiver computer. The Examiner (page 3, lines 10-14) correctly points out that McMillan fails to teach step c, sending an email containing a hypertext link referencing the document file. It follows that McMillan therefore also fails to teach steps d and e, since each of these steps either relate to transmitting a document file in response to a hypertext link activation or displaying in a browser window a document received in response to a hypertext link activation. The Examiner (page 4, lines 1-2) also correctly points out that McMillan fails to teach step f.

The Examiner cites Clark (col. 7, lines 5-25) as teaching step f. Clark (col. 1, line 65 through col. 2, line 1) teaches a "Document Relational Service" that notifies an "originator" when a "recipient" has accessed an "isochronous mail object" for a specified amount of time. Clark does not directly define an "isochronous mail object" but (at col. 1, lines 41-43) defines "transmissions of isochronous data" as "transmissions of time-dependant data such as real-time video and digital voice". Clark (col. 1, lines 37-41) implies that an "isochronous mail object" is an object embedded in email that causes a receiver computer to display a real-time video, audio or other time-varying media presentation. Clark (col. 5, lines 4-19) teaches that when the receiver accesses isochronous objects conveyed in an email it generate the presentation and to also initiates a "time service monitor". When the presentation described by each isochronous object completes after having run for a specified time, the time service monitor sends an acknowledgment to the sender computer (col. 5, lines 45-49).

One of skill in the art would be motivated to apply the teachings of Clark to McMillan, since McMillan teaches to embed code in email that produces a media presentation on a recipient's computer when the recipient opens the email. Accordingly, the combination of McMillan and Clark would motivate one to provide the following media delivery method, with steps ordered and numbered to track steps of claim 1 as closely as possible:

a. generating a media file describing a media presentation on a sender computer,

b. sending the media file from the sender computer to the server computer;

c. embedding an isochronous object (code) in an email message , and sending the email from the server to a receiver computer,

d. (no step)

e. automatically executing the isochronous object on the receiver computer to generate the media presentation, and

f. sending verification data from the receiver computer to the server computer indicating that the receiver computer has successfully produced the media presentation generated by the code embedded in an email.

Note that since nothing in the combined McMillan/Clark method relates to sending a document file in response to hypertext link activation, there is no equivalent step d of the McMillan/Clark method. McMillan and Clark therefore fail to teach step d of claim 1. Steps c, e and f also differ from claim 1 in that they do not relate to email containing a hypertext link, to sending a document file in response to a hyperlink activation, or to processing a document file received in this fashion to produce an image of a document in a browser window.

The Examiner (page 3, lines 10-17) cites Linden as teaching to embed a hypertext link in an Email that a receiver may activate to obtain a document file from a server. The Examiner (page 3, lines 17-21) correctly observes that one of skill in the art would be motivated to substitute Linden's hypertext link approach to delivering content for the embedded executable code approach taught by McMillan and Clark because, as the Examiner points out, executable objects embedded in email can cause "virus infection and unwanted executing of scripts". The Examiner (page 3, lines 19-21 concludes that in view of the dangers of such embedded code, one of ordinary skill in the art would be motivated to "[disallow] executable programs [that] launch automatically" from being included in emails. It follows then, that one of skill in the art would be motivated to "disallow" any step in the combined McMillan/Clark/Linden method involving embedded executable code. The combined McMillan/Clark/Linden system would presumably look as follows:

a. generating a media file describing a media presentation on a sender computer,

b. sending the media file from the sender computer to the server computer;

c. sending email) to a receiver computer containing a hypertext link that the receiver activates to send a reference to the media file to the server computer,

d. sending the media file from the server computer to the receiver computer after the server computer receives the reference to the document file from the receiver computer, and

e. processing the media file sent to the receiver computer to generate a display of the media presentation.

The combined McMillan/Clark/Linden method <u>fails to include step f</u> of claim 1. Linden teaches that if a server wants a receiver computer to produce a media display and then return verification data indicating that it has done so, the server must send executable code to the receiver in email causing the receiver computer to generate the media display and return the verification data. However, if the server sends an email containing only a hypertext link to a document file, and subsequently sends the document file to the browser program in the receiver when the receiver activates the hypertext link, it is the receiver's browser program, rather than any executable code sent by the server, that controls the actions the receiver carries out after it receives the document file. While conventional browser programs are adapted to display documents in browser windows, they are not adapted to send acknowledgment data to a server after successfully displaying a document in a browser window.

It is novel and inventive to adapt a receiver computer to automatically send an acknowledgment to a server when its browser program has received a document file in response a hyperlink activation and then successfully displayed the document in a browser window. There is no teaching in any of the cited references that a receiver computer can or should be so adapted.

The applicant's claim 1 is therefore patentable over the combination of McMillan, Clark and Linden.

Claims 4, 5-8, 14 - 17 and 21 are patentable over the combination of McMillan, Clark and Linden for reasons expressed above in connection with claim 1.

Claim 2

Claim 2 depends on claim 1 and is patentable over the combination of McMillan, Clark and Linden for reasons expressed above in connection with claim 1. Claim 2 further recites a step of storing log data on the server indicating when the receiver returned the verification data. The Examiner cites McMillan's FIG. 13, step 410 and col. 9, line 15-52 as teaching this, but none of the cited sections of McMillan relate to a client computer storing log data indicting when the receiver has returned verification data.

Claim 13

Claim 13 depends on claim 1 and is patentable over the combination of McMillan, Clark and Linden for similar reasons. Claim 13 further recites "the receiver computer returns the verification data to the server computer as an encoded network address." The

Examiner cites McMillan, col. 9, lines 15-52 as teaching the additional subject matter of claim 13, however nothing in this section of McMillan teaches anything about a receiver computer returning verification data to the server computer that the receiver computer has successfully displayed a document described by a document file delivered in response to activation of a hypertext link or provides any teaching that any verification of any activity by any computer should be transmitted to a server computer in the form of an encoded network address.

2. **Arguments against rejection of claims 9, 10, and 20 rejected under 35 U.S.C. 103(a) as being unpatentable over the combination McMillan, Linden, Clark and Ohashi.**

Claims 9 and 20

The Examiner relies on the combination of McMillan, Linden and Clark as teaching the underlying subject matter of the parent claim 1 of claim 9 and relies on Ohashi as teaching the additional subject matter of claim 9. Claim 9 is patentable over the combination of McMillan, Linden, Clark and Ohashi because they fail to teach step f of claim 1. Claim 9 also recites that the sender transmits a publish request to the server identifying the receiver and indicating that the "receiver computer is to be prevented from sending the document file to a printer". The Examiner cites Ohashi (Abstract) as disclosing a mechanism by which a receiver computer is prevented from performing a print screen operation when displaying an image of document in a browser; however a print screen operation and sending a document file to a printer are two different activities. Preventing a computer from performing a print screen operation does not prevent it from sending a print file to a printer.

In a print screen operation, an image of that which is displayed on a screen is printed or copied to a clip board. Though a receiver computer may display all or a portion of a document described by a document file (such as an html file) on a screen, a print screen command does not send the document file itself to the printer. A print screen command creates a new print file describing only what appears on the screen on a pixel-by-pixel basis and then sends that new print file to the printer. Assume, as contemplated by Ohashi, a browser running on a computer is generating an image of a document such as a web page described by a document file such as an HTML file. A computer generates a display of the browser window and as much of the document as can fit in the window as an array of pixels on a display monitor. In a print screen operation, the computer creates another file that indicates in a language the printer can understand, the position, intensity and color of each pixel, and sends that file to the printer causing the printer to as nearly as possible print an image of what appears on the screen. What is printed will only be a part of a document if not all of the document is currently displayed in the browser window, and will include things other than the document that may also be displayed on the screen, such as the window frame of the browser and any other items that happen to be displayed on the screen. Note that when carrying out a print screen operation while displaying a part or all of a document described by a document file, the computer does not send the document file itself to the printer and does not even consult the document file. It only creates a new file based on the current state of the display and sends that to the printer. Thus preventing a computer from carrying out a print screen operation does not mean that the computer is prevented from forwarding to a printer a document file it has received from a server, when that document file happens to be formatted as a print file.

Document delivery systems normally transmit documents files in a form which cannot be directly understood by a printer such as a word processing, a graphics or HTML file. Software in a receiving computer must first convert the document file into a print file that the printer can understand, and then send the print file to the printer. The printer then prints an image of the entire document and nothing else. In accordance with the applicant's document delivery method as recited in claims 9, a sender transmits a print file via a server to a receiver, and view software generates a display based on the print file. In accordance with claims 9, the document sender can provide a publication request indicating that the receiver computer is to be prevented from sending that print file to a printer.

Ohashi (abstract and col. 2, lines 10-18) teaches to prevent a computer from carrying out a print screen operation when the computer is displaying an image that includes part or all of a document described by a document file, but nothing in Ohashi teaches to prevent a computer from sending the document file itself to the printer when the document file is in the form of a print file. Ohashi does not contemplate that the document file might itself be a print file that could be sent to a printer. Thus Ohashi' teaching provide incomplete protection against making unauthorized hard copies of a document described by a document file. Note also the programming needed to prevent a computer from carrying out a print screen operation is very much different that the programming needed to prevent a computer from forwarding to a printer a particular print file it has received from a server.

The Examiner's discussion of "encapsulation packages" taught by McMillan (col. 4, lines 48-59) is not particularly relevant to the subject matter of claim 9 since claim 9 does not recite encapsulation packages or anything that can be considered to be an encapsulation package. Also, neither Ohashi nor McMillan say anything about using "encapsulation packages" to prevent a receiver from sending a document file to a printer. McMillan speaks of using encapsulation packages only to make content such as document files more accessible and useful to receiver computers, not less accessible and useful.

The Examiner's discussion of Ohashi's teaching to "reduce tendencies of unauthorized user obtaining classified or internal information" is not relevant to claim 9, since claim 9 does not recite preventing unauthorized users from obtaining information. Claim 9 recites preventing a receiver computer from sending a document file to a printer.

Claim 20 is patentable over the combination of combination McMillan, Linden, Clark and Ohashi for reasons similar to those expressed above in connection with claim 9. The Examiner's comments regarding claim 20 do not relate to the subject matter of the current version of claim 20.

Claims 10

Claim 10 depends on claim 9 and is patentable over the combination of McMillan, Linden, Clark and Ohashi for reasons cited above in connection with claim 9. Also none of these references teach a method in which a sender computer supplies a compressed print file as a document file to be forward to a receiver computer via a server computer, decompresses the document file at the receiver computer to reproduce the print file, and then generates a display of the document described by the print file as recited in claim 10. The Examiner's comments regarding claim 10 do not relate to the subject matter of the current version of claim 10.

3. Arguments against rejection of claims 11, 12, 18 and 19 should be rejected under 35 U.S.C. 103(a) as being unpatentable over McMillan, Linden, Clark and Kurokawa.

Claims 11 and 12, 18 and 19

The Examiner relies on McMillan, Linden, Clark as teaching the subject matter of the parent claims 1 or 14 of claims 11 and 12 or 18 and 19, and relies on Kurokawa only as teaching the additional subject matter of claims 11 and 12. Claims 11 and 12 are patentable over the combination of McMillan, Linden, Clark and Kurokawa since, as discussed above, McMillan, Linden, and Clark fail to teach step f of claim 1 or 14 and because Kurokawa fails to teach step f.

Claims Appendix

1. A method for transmitting a document from a sender computer to a receiver computer via a computer network linking the sender computer and the receiver computer to a server computer, wherein the sender computer is operated by a sender, wherein the receiver computer is operated by a receiver, the method comprising the steps of:

a. generating a document file describing the document on the sender computer;

b. sending the document file from the sender computer to the server computer;

c. sending email to the receiver computer containing a hypertext link that the receiver activates to send a reference to the document file to the server computer;

d. sending the document file from the server computer to the receiver computer after the server computer receives the reference to the document file from the receiver computer;

e. processing the document file sent to the receiver computer to generate a display of an image of the document in a browser window on the receiver computer; and

f. sending verification data from the receiver computer to the server computer indicating that the receiver computer has successfully displayed the image of the document in the browser window.

2. The method in accordance with claim 1 further comprising the steps of:

g. storing log data on the server computer indicating when the receiver computer returned the verification data to the server computer indicating that the receiver computer has successfully displayed in the browser window the image of the document referenced by the hypertext link; and

h. providing the sender computer with access to the log data via the computer network.

3. The method in accordance with claim 1 further comprising the steps of:

g. transmitting a comment file containing comments generated by the receiver from the receiver computer to the server computer, wherein the comment file references the document file;

h. storing the comment file on the server computer; and

i. providing the sender computer with access to the comment file via the computer network.

4. The method in accordance with claim 1 further comprising the step of:

g. transmitting a publish request from the sender computer to the server computer wherein the publish request identifies the receiver computer.

5. The method in accordance with claim 4 further comprising the step of:

h. storing the document file in the server computer and assigning a network address to the document file stored on the server computer, wherein the hypertext link references the assigned network address.

6. The method in accordance with claim 1 further comprising the step of:

g. sending a document password entry form from the server computer to the receiver computer after the server computer receives the reference to the document file from the receiver computer, wherein the receiver enters into the document password entry form a document password associated with the document that the receiver computer sends to the server computer prior to step d.

7. The method in accordance with claim 6 further comprising the step of:

h. sending a user sign-in form from the server computer to the receiver after the server computer receives the reference to the document file from the receiver computer at step c, wherein the user enters into the sign-in form a user name and a user password that the receiver computer sends to the server computer prior to step d.

8. The method in accordance with claim 1 wherein step a comprises generating on the sender computer a print file for directing a printer to print the document, and processing the print file to generate the document file.

9. The method in accordance with claim 1 wherein the document file is a print file and the method further comprising the step of:

g. transmitting a publish request from the sender computer to the server computer, wherein the publish request identifies the receiver computer, wherein the publish request indicates that the receiver computer is to be prevented from sending the document file to a printer.

10. The method in accordance with claim 9 wherein step a comprises generating on the sender computer a print file for directing a printer to print the document, and then compressing the print file to generate the document file and

wherein step e comprises decompressing the document file to produce the print file and then processing the print file to generate the display of the image of the document in the browser window on the receiver computer.

11. The method in accordance with claim 1 further comprising the steps of:

g. assigning to the document file a document password generated by the sender, and

h. transmitting the document password to the server computer.

12. The method in accordance with claim 11 further comprising the steps of:

i. providing a document password entry form to the receiver computer in which the receiver enters the document password,

j. conveying the document password entered into the document password entry form to the server computer, and

wherein step g is carried out only after the server computer receives the document password from the receiver computer.

13. The method in accordance with claim 1 wherein the receiver computer returns the verification data to the server computer as an encoded network address.

14. A method for transmitting a document file describing a document from a sender computer to a receiver computer via a computer network linking the sender computer and the receiver computer to a server computer, wherein the sender computer is operated by a sender, wherein the receiver computer is operated by a receiver, wherein the receiver computer includes a monitor viewable by the receiver, the method comprising the steps of:

a. transmitting the document file via the computer network from the sender computer to the server computer;

b. storing the document file on the server computer and assigning the document file a unique network address;

c. transmitting an email message via the computer network to the receiver computer, wherein the email message includes a hypertext link to the document files assigned network address;

d. displaying the email message on the receiver computer monitor so that the receiver may view it and activate the hypertext link whereby the receiver computer returns the document file's network address to the server computer;

e. transmitting the document file from the server computer to the receiver computer via the computer network following the receiver's activation of the hypertext link; and

f. providing viewer software running on the receiver computer for generating a display on the receiver computer monitor of the document described by the document file when received by the receiver computer;

wherein when the viewer software has successfully displayed the document, it automatically returns verification data in the form of an encoded network address to the server computer via the computer network verifying that the document has been successfully displayed.

15. The method in accordance with claim 14 further comprising the step of:

g. prior to step a, transmitting a publish request from the sender computer to the server computer wherein the publish request identifies the receiver that is to receive the email message at step c.

16. The method in accordance with claim 15 wherein the publish request transmitted in step g indicates that the receiver must sign on to the server computer by transmitting, prior to step e, a user name and a user password to the server computer via the computer network in order to receive the document file at step e.

17. The method in accordance with claim 16 wherein step e comprises the sub-steps of:

e1. verifying that the receiver is signed on to the server computer, and

e2. thereafter transmitting the document file from the server computer to the receiver computer via the computer network following the receiver's activation of the hypertext link.

18. The method in accordance with claim 17 further comprising the steps of:

h. assigning to the document file a document password generated by the sender; and

i. prior to step b, transmitting the document password to the server computer.

19. The method in accordance with claim 18 wherein step e comprises the substeps of:

e1. providing a document password entry form to the receiver computer in which the receiver enters the document password;

e2. conveying the document password entered into the document password entry form from the receiver computer to the server computer; and e3. transmitting the document file from the server computer to the receiver computer via the computer network at step e only after the server computer receives the document password from the receiver computer.

20. The method in accordance with claim 15 wherein the document file is a print file and wherein the publish request indicates whether the receiver computer is to be prevented from sending the document file to a printer.

21. The method in accordance with claim 14 further comprising the steps of:

g. storing log data on the server computer indicating when the receiver computer returned the verification data to the server computer; and

h. providing the sender computer with access to the log data via the computer network.

22. The method in accordance with claim 14 further comprising the steps of:

g. transmitting a comment file containing comments generated by the receiver from the receiver computer to the server computer, wherein the comment file references the document file;

h. storing the comment file on the server computer; and

i. providing the sender computer with access to the comment file via the computer network.

Evidence Appendix

Not applicable.

Related Proceedings Appendix

Not Applicable.

Respectfully submitted,

Daniel J. Bedell
Reg. No. 30,156

SMITH-HILL & BEDELL, P.C.
16100 N.W. Cornell Road, Suite 220
Beaverton, Oregon 97006

Tel. (503) 574-3100
Fax (503) 574-3197
Docket: SWIF 2123
Postcard: 05/06-19

Certificate of Mailing or Transmission

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, or facsimile transmitted to the U.S. Patent and Trademark Office, on the 19 day of May, 2006.

Penelope Stockwell